

BILINEAR FORMS WITH EXPONENTIAL SUMS WITH BINOMIALS

KUI LIU, IGOR E. SHPARLINSKI, AND TIANPING ZHANG

ABSTRACT. We obtain several estimates for bilinear form with exponential sums with binomials $mx^k + nx^\ell$. In particular we show the existence of nontrivial cancellations between such sums when the coefficients m and n vary over rather sparse sets of general nature.

1. INTRODUCTION

1.1. Background and motivation. For a positive integer q , we denote by \mathbb{Z}_q the residue ring modulo q and also denote by \mathbb{Z}_q^* the group of units of \mathbb{Z}_q .

For fixed integers k and ℓ , we consider exponential sums with binomials

$$S_{k,\ell,q}(m,n) = \sum_{x \in \mathbb{Z}_q^*} \mathbf{e}_q(mx^k + nx^\ell),$$

where for negative k or ℓ the inversion of x is computed modulo q and

$$\mathbf{e}_q(z) = \exp(2\pi iz/q).$$

The case $(k, \ell) = (1, -1)$ corresponds to the case of Kloosterman sums.

Furthermore, given two sets $\mathcal{M}, \mathcal{N} \subseteq \mathbb{Z}_q$ and two sequences of weights $\mathcal{A} = \{\alpha_m\}_{m \in \mathcal{M}}$ and $\mathcal{B} = \{\beta_n\}_{n \in \mathcal{N}}$, we define the bilinear sums of binomial sums

$$\mathcal{S}_{k,\ell,q}(\mathcal{A}, \mathcal{B}; \mathcal{M}, \mathcal{N}) = \sum_{m \in \mathcal{M}} \sum_{n \in \mathcal{N}} \alpha_m \beta_n S_{k,\ell,q}(m, n).$$

We also consider the following special cases

$$\begin{aligned} \mathcal{S}_{k,\ell,q}(\mathcal{A}; \mathcal{M}, \mathcal{N}) &= \mathcal{S}_{k,\ell,q}(\mathcal{A}, \{1\}_{n \in \mathcal{N}}; \mathcal{M}, \mathcal{N}) \\ (1.1) \quad &= \sum_{m \in \mathcal{M}} \sum_{n \in \mathcal{N}} \alpha_m S_{k,\ell,q}(m, n), \end{aligned}$$

2010 *Mathematics Subject Classification.* 11D79, 11L07.

Key words and phrases. Binomial sums, cancellation, bilinear form.

T. P. Zhang is the corresponding author (tpzhang@snnu.edu.cn).

and

$$(1.2) \quad \begin{aligned} \mathcal{S}_{k,\ell,q}(\mathcal{M}, \mathcal{N}) &= \mathcal{S}_{k,\ell,q}(\{1\}_{m \in \mathcal{M}}, \{1\}_{n \in \mathcal{N}}; \mathcal{M}, \mathcal{N}) \\ &= \sum_{m \in \mathcal{M}} \sum_{n \in \mathcal{N}} S_{k,\ell,q}(m, n). \end{aligned}$$

For $(k, \ell) = (1, -1)$, that is, for Kloosterman sums, such bilinear forms have been introduced by Fouvry, Kowalski and Michel [4] who have also demonstrated the importance of estimating them beyond of what follows immediately from the Weil bound, see [9, Chapter 11], which is essentially given by (1.3) below.

More generally, for arbitrary modulus q and exponents (k, ℓ) one can apply the general bound of [18, Theorem 1] on exponential sums with few nomials to derive

$$(1.3) \quad |\mathcal{S}_{k,\ell,q}(\mathcal{A}, \mathcal{B}; \mathcal{M}, \mathcal{N})| \leq MNq^{1/2+o(1)} \max_{m \in \mathcal{M}} |\alpha_m| \max_{n \in \mathcal{N}} |\beta_n|,$$

to which we refer as the *trivial bound*.

Further progress in the case $(k, \ell) = (1, -1)$ has been achieved in [1, 2, 12, 19, 20]. In [23] this question has been studied on average over the moduli q . We also recall recent results of [11, 13, 22] when cancellations among Kloosterman sums are studied for moduli of special arithmetic structure. Furthermore, in the case of a prime $q = p$ and $(k, \ell) = (2, -1)$ has been studied by Nunes [14], via the method of Fouvry, Kowalski and Michel [4]. Then these sums have been used to investigate the distribution of squarefree integers in arithmetic progressions; see Section 5 for exact formulations of the results of Nunes [14] and their comparison with our bounds.

We remark that the method introduced by Fouvry, Kowalski and Michel [4], and then further developed and used in [1, 12, 14], relies heavily on such deep tools as the Weil and Deligne bounds, see [9, Chapter 11]. In particular, this approach works well only for prime moduli p . It is important to note the methods of [19, 20] are of elementary nature, and in particular work without any losses of strength for composite q as well. On the other hand, the method of [1, 4, 12, 23] works for much more general objects than Kloosterman and other similar exponential sums.

1.2. General notation. We remark that our bounds involve only the norms of the weights \mathcal{A} but do not explicitly depend on the size of the set \mathcal{M} on which they are supported. Hence, without loss of generality, we can assume that $\mathcal{M} = \mathbb{Z}_q$. On the other hand, our method does not apply to general sets \mathcal{N} and works only when \mathcal{N} is an interval,

and thus, for the sums with weights we simplify the notation as

$$(1.4) \quad \mathcal{S}_{k,\ell,q}(\mathcal{A}, \mathcal{B}; \mathcal{J}) = \sum_{m \in \mathbb{Z}_q} \sum_{n \in \mathcal{J}} \alpha_m \beta_n S_{k,\ell,q}(m, n),$$

and even further as

$$(1.5) \quad \mathcal{S}_{k,\ell,q}(\mathcal{A}; \mathcal{J}) = \sum_{m \in \mathbb{Z}_q} \sum_{n \in \mathcal{J}} \alpha_m S_{k,\ell,q}(m, n),$$

where $\mathcal{J} = \{L+1, \dots, L+N\} \subseteq \mathbb{Z}_q$ is a set of N consecutive residues of \mathbb{Z}_q (with $q-1$ followed by 0). Furthermore, in the case of the sums without weights we only estimate such sums when the set $\mathcal{M} = \mathcal{I} = \{K+1, \dots, K+M\} \subseteq \mathbb{Z}_q$ is another interval, and thus we write $\mathcal{S}_{k,\ell,q}(\mathcal{I}, \mathcal{J})$.

The case of $\ell = -1$ is somewhat special as it admist some extra treatment and is also important for many applications, see [14] for example. Thus we introduce special notation

$$(1.6) \quad \begin{aligned} \mathcal{S}_{k,q}^*(\mathcal{A}, \mathcal{B}; \mathcal{J}) &= \mathcal{S}_{k,-1,q}(\mathcal{A}, \mathcal{B}; \mathcal{J}), \\ \mathcal{S}_{k,q}^*(\mathcal{A}; \mathcal{J}) &= \mathcal{S}_{k,-1,q}(\mathcal{A}; \mathcal{J}), \\ \mathcal{S}_{k,q}^*(\mathcal{I}, \mathcal{J}) &= \mathcal{S}_{k,-1,q}(\mathcal{I}, \mathcal{J}). \end{aligned}$$

For an integer u we define

$$\langle u \rangle_q = \min_{k \in \mathbb{Z}} |u - kq|$$

as the distance to the closest integer, which is a multiple of q .

We also define the norms

$$\|\mathcal{A}\|_\infty = \max_{m \in \mathcal{M}} |\alpha_m| \quad \text{and} \quad \|\mathcal{A}\|_\sigma = \left(\sum_{m \in \mathcal{M}} |\alpha_m|^\sigma \right)^{1/\sigma},$$

where $\sigma > 0$, and similarly for the weights \mathcal{B} .

Throughout the paper, as usual $A \ll B$ is equivalent to the inequality $|A| \leq cB$ with some constant $c > 0$, which may depend on the integers k and ℓ , and occasionally, where obvious, the real parameter $\varepsilon > 0$ and on the integer parameter $\nu \geq 1$.

The letter p always denotes a prime number and we say that q is *squarefree* if it not divisible by p^2 for any p .

2. NEW RESULTS

2.1. Bounds for every q . We start with the sums $\mathcal{S}_{k,\ell,q}(\mathcal{A}; \mathcal{J})$, defined in (1.5), which are medium level of complexity as one variable still runs through a continuous interval. The proof is based on the method from [20], coupled with a result of Pierce [16, Theorem 4]

Theorem 2.1. *If $k \neq \ell$ are fixed nonzero integers with $\gcd(k, \ell) = 1$, then, for any fixed positive integer ν , squarefree $q \geq 1$ and*

$$\mathcal{J} = \{L + 1, \dots, L + N\} \subseteq \mathbb{Z}_q,$$

we have

$$\begin{aligned} \mathcal{S}_{k,\ell,q}(\mathcal{A}; \mathcal{J}) &\ll \min \left\{ \|\mathcal{A}\|_2 N^{1/2} q, \|\mathcal{A}\|_1^{1-1/\nu} \|\mathcal{A}\|_2^{1/\nu} \right. \\ &\quad \left. \left(q + q^{(2\nu^2+\nu+1)/2\nu(\nu+1)} N^{1/(\nu+1)} \right) q^{o(1)} \right\}. \end{aligned}$$

In particular, when α_m is the characteristic function of the interval $\mathcal{I} = \{K + 1, \dots, K + M\}$ we obtain a bound on the sums $\mathcal{S}_{k,\ell,q}(\mathcal{I}, \mathcal{J})$, defined by (1.2). We also see that in the case of the sums $\mathcal{S}_{k,\ell,q}(\mathcal{I}, \mathcal{J})$ the roles of M and N can be interchanged.

Corollary 2.2. *If $k \neq \ell$ are fixed nonzero integers with $\gcd(k, \ell) = 1$, then, for any fixed positive integer ν , squarefree $q \geq 1$ and*

$$\mathcal{I} = \{K + 1, \dots, K + M\}, \quad \mathcal{J} = \{L + 1, \dots, L + N\} \subseteq \mathbb{Z}_q,$$

we have

$$\mathcal{S}_{k,\ell,q}(\mathcal{I}, \mathcal{J}) \leq X^{1-1/2\nu} \left(q + q^{(2\nu^2+\nu+1)/2\nu(\nu+1)} Y^{1/(\nu+1)} \right) q^{o(1)}$$

for any choice of X, Y with $\{X, Y\} = \{M, N\}$.

In particular, with $\nu = 2$ we obtain from Corollary 2.2 that

$$(2.1) \quad \mathcal{S}_{k,\ell,q}(\mathcal{I}, \mathcal{J}) \leq q^{1+o(1)} N^{3/4} + q^{11/12+o(1)} M^{1/3} N^{3/4}.$$

This improves the trivial bound (1.3) provided that

$$(2.2) \quad M^4 N \geq q^{2+\varepsilon} \quad \text{and} \quad M^8 N^3 \geq q^{5+\varepsilon}$$

for some fixed $\varepsilon > 0$, and in particular for $M = N \geq q^{5/11+\varepsilon}$. Note that in (2.1) and (2.2) the roles of M and N can be interchanged.

In the case $M, N = q^{1/2+o(1)}$ crucial for many applications, Corollary 2.2 implies the bound $MNq^{1/2-1/24+o(1)}$, saving $q^{1/24}$ compared to the trivial bound (1.3).

Finally, we estimate the sum $\mathcal{S}_{k,q}^*(\mathcal{A}, \mathcal{B}; \mathcal{J})$, see (1.4) and (1.6), which is the most complicated case that requires some extra arguments combined with the ideas of [19, 20].

Theorem 2.3. *If $k > 1$ is a fixed integer, then, for any fixed positive integer ν , prime $p \geq 1$ and*

$$\mathcal{J} = \{L + 1, \dots, L + N\} \subseteq \mathbb{Z}_p,$$

we have

$$\mathcal{S}_{k,p}^*(\mathcal{A}, \mathcal{B}; \mathcal{J}) \leq \sqrt{\|\mathcal{A}\|_2 \|\mathcal{B}\|_2} (p^{(6\nu-1)/4\nu} + p^{(3\nu+2)/2(\nu+1)} N^{1/2(\nu+1)}) p^{o(1)}.$$

2.2. Bounds for almost all q . We also show that in the case of $\ell = 1$ for almost all q in a dyadic interval $[Q, 2Q]$ stronger versions of the results of Section 2.1 hold.

We also have an analogue of the second bound in Theorem 2.1, but only for the sums $\mathcal{S}_{k,q}^*(\mathcal{A}; \mathcal{J})$.

Theorem 2.4. *If $k > 1$ is a fixed integer, then, for any fixed positive integer ν , fixed real $\varepsilon > 0$ and sufficiently large real $Q \geq 1$, for all but $O(Q^{1-\varepsilon})$ integers $q \in [Q, 2Q]$, we have*

$$\mathcal{S}_{k,q}^*(\mathcal{A}; \mathcal{J}) \ll \|\mathcal{A}\|_1^{1-1/\nu} \|\mathcal{A}\|_2^{1/\nu} (q + q^{(\nu+1)/2\nu} N^{1/2}) q^\varepsilon.$$

We now have the following version of Corollary 2.2 (however this time we cannot interchange the roles of M and N).

Corollary 2.5. *If $k > 1$ is a fixed integer, then, for any fixed positive integer ν , fixed real $\varepsilon > 0$ and sufficiently large real $Q \geq 1$, for all but $O(Q^{1-\varepsilon})$ integers $q \in [Q, 2Q]$, we have*

$$\mathcal{S}_{k,q}^*(\mathcal{I}, \mathcal{J}) \ll M^{1-1/2\nu} (q + q^{(\nu+1)/2\nu} N^{1/2}) q^\varepsilon.$$

3. PREPARATIONS

3.1. Linear and bilinear exponential sums. We need the following well-known simple results.

First we recall the following bound of linear sums [9, Bound (8.6)].

Lemma 3.1. *For any integers u , L and $N \geq 1$, we have*

$$\sum_{n=L+1}^{L+N} \mathbf{e}_q(nu) \ll \min \left\{ N, \frac{q}{\langle u \rangle_q} \right\}.$$

We also need the following well-known result, which dates back to Vinogradov [24, Chapter 6, Problem 14.a].

Lemma 3.2. *For arbitrary set $\mathcal{U}, \mathcal{V} \subseteq \mathbb{Z}_q$ and complex numbers φ_u and ψ_v with*

$$\sum_{u \in \mathcal{U}} |\varphi_u|^2 \leq \Phi \quad \text{and} \quad \sum_{v \in \mathcal{V}} |\psi_v|^2 \leq \Psi,$$

we have

$$\left| \sum_{u \in \mathcal{U}} \sum_{v \in \mathcal{V}} \varphi_u \psi_v \mathbf{e}_q(uv) \right| \leq \sqrt{\Phi \Psi q}.$$

3.2. Some equations and congruences. We start with a very simple result on the monomial congruences.

Lemma 3.3. *If k is a nonzero integer then for any $a \in \mathbb{Z}_q$ the congruence*

$$x^k \equiv a \pmod{q}, \quad x \in \mathbb{Z}_q^*,$$

has at most $q^{o(1)}$ solutions.

Proof. Clearly we can assume that $a \in \mathbb{Z}_q^*$ as otherwise there is no solution. Then the discriminant of the polynomial $X^k - a$ has a bounded greatest common divisor with q and the result follows from the general bound of Huxley [8]. \square

We also need several results of Pierce [16], which in turn generalises previous results of Heath-Brown [Lemma 1][7] (which corresponds to $\ell = -1$). We present these results in slightly more general forms (which are however implicitly contained in the argument of [16]).

For an integer $\nu \geq 1$ and real U let $I_{k,\ell,\nu,q}(U)$ be the number of solutions to the system of congruences

$$\begin{aligned} v_1 + \dots + v_\nu &\equiv v_{\nu+1} + \dots + v_{2\nu} \pmod{q}, \\ u_i^k &\equiv v_i^\ell \pmod{q}, \quad i = 1, \dots, 2\nu, \end{aligned}$$

with $1 \leq u_1, \dots, u_{2\nu} \leq U$ and unrestricted variables $v_1, \dots, v_{2\nu} \in \mathbb{Z}_q$. We have the following slight extension of the bound of Pierce [16, Equation (6.2)] (which is free of the restriction $U \leq q^{(\nu+1)/2\nu}$).

We recall that all implied constants are allowed to depend on ν .

Lemma 3.4. *If $k \neq \ell$ are fixed nonzero integers with $\gcd(k, \ell) = 1$, then, for any fixed positive integer ν , squarefree $q \geq 1$ and $U \leq q$ we have*

$$I_{k,\ell,\nu,q}(U) \leq \left(U^{2\nu} q^{-1} + U^{2\nu^2/(\nu+1)} \right) q^{o(1)}.$$

Proof. We use the following inequality given (in a slightly more precise form) in [16, Section 6.3]:

$$I_{k,\ell,\nu,q}(U) \leq (Q^{-1} U^{2\nu-1} + Q^\nu U^\nu) q^{o(1)},$$

holds for any Q , satisfying the conditions

$$Q < U \quad \text{and} \quad 8QU \leq q.$$

Thus taking

$$Q = \min \left\{ U^{(\nu-1)/(\nu+1)}, q/8U \right\},$$

we obtain the result. \square

Furthermore, for $\ell = -1$ and prime $q = p$, Bourgain and Garaev [3, Proposition 1] extend Lemma 3.4 to solutions in intervals away from the origin. For a real U and W let $I_{k,\nu,q}^*(U, W)$ be the number of solutions to the system of congruences

$$\begin{aligned} \frac{1}{u_1^k} + \dots + \frac{1}{u_\nu^k} &\equiv \frac{1}{u_{\nu+1}^k} + \dots + \frac{1}{u_{2\nu}^k} \pmod{q}, \\ W + 1 &\leq u_1, \dots, u_{2\nu} \leq W + U. \end{aligned}$$

Then, by [3, Proposition 1] we have the following estimate

Lemma 3.5. *If $k > 1$ is a fixed integer, then, for any fixed positive integer ν , prime $p \geq 1$ and $U \leq p$ we have*

$$I_{k,\nu,p}^*(W, U) \leq \left(U^{2\nu} p^{-1} + U^{2\nu^2/(\nu+1)} \right) p^{o(1)}.$$

In the case $\ell = -1$, following our previous convention, we denote

$$I_{k,\nu,q}^*(U) = I_{k,-1,\nu,q}(U).$$

We now show that one can get a better bound on $I_{k,\nu,q}^*(U)$ and thus on $T_{k,q}^*(U)$ on average over q in a dyadic interval $[Q, 2Q]$.

Indeed, let $J_{k,\nu}(U)$ be the number of solutions to the equation

$$(3.1) \quad \frac{1}{u_1^k} + \dots + \frac{1}{u_\nu^k} = \frac{1}{u_{\nu+1}^k} + \dots + \frac{1}{u_{2\nu}^k}, \quad 1 \leq u_1, \dots, u_{2\nu} \leq U.$$

We have the following bound, which is a slight modification of a result of Karatsuba [10], corresponding to $k = 1$ and presented in the proof of [10, Theorem 1]).

Lemma 3.6. *If $k > 1$ is a fixed integer, then, for any fixed positive integer ν , we have*

$$J_{k,\nu}(U) \leq U^{\nu+o(1)}.$$

Proof. Clearing the denominators in (3.1) we see that if $p \mid u_i$ for some component $i = 1, \dots, 2\nu$ of a solution, then we also have $p \mid u_j$ for some $j \neq i$. This means that for any solution to (3.1), the product $u_1 \dots u_{2\nu}$ is squarefull. Since any interval $[1, W]$ contains $O(W^{1/2})$ squarefull integers, see [21], applying this with $W = U^{2\nu}$ and then using the classical bound on the divisor function, see [9, Equation (1.81)], we obtain the result. \square

Now repeating the argument of the proof of [5, Lemma 2.3] and using Lemma 3.6 in the appropriate place, we obtain:

Lemma 3.7. *If $k > 1$ is a fixed integer, then, for any fixed positive integer ν and sufficiently large real $1 \leq U \leq Q$, we have*

$$\frac{1}{Q} \sum_{Q \leq q \leq 2Q} I_{k,\nu,q}^*(U) \leq (U^{2\nu} Q^{-1} + U^\nu) Q^{o(1)}.$$

Using Lemma 3.7 for every $U_i = e^i$, $i = 1, \dots, \lceil \log(2Q) \rceil$, (where $e = 2.7182\dots$ is the base of the natural logarithm) we immediately derive:

Corollary 3.8. *If $k > 1$ is a fixed integer, then, for any fixed positive integer ν , real positive $\varepsilon > 0$ and sufficiently large real $Q \geq 1$, for all but $O(Q^{1-\varepsilon})$ integer $q \in [Q, 2Q]$, we have*

$$I_{k,\nu,q}^*(U) \leq (U^{2\nu} Q^{-1} + U^\nu) Q^{\varepsilon+o(1)}$$

for every $U \leq q$.

4. PROOFS MAIN RESULTS

4.1. Proof of Theorem 2.1. Changing the order of summation, we obtain

$$\mathcal{S}_{k,\ell,q}(\mathcal{A}; \mathcal{J}) = \sum_{x \in \mathbb{Z}_q^*} \sum_{m \in \mathcal{I}} \alpha_m \mathbf{e}_q(mx^k) \sum_{n \in \mathcal{J}} \mathbf{e}_q(nx^\ell).$$

Recalling Lemma 3.1, we obtain

$$\mathcal{S}_{k,\ell,q}(\mathcal{A}; \mathcal{J}) = \sum_{m \in \mathbb{Z}_q} \sum_{x \in \mathbb{Z}_q^*} \alpha_m \gamma_x \mathbf{e}_q(mx^k),$$

where

$$|\gamma_x| \leq \min \left\{ N, \frac{q}{\langle x^\ell \rangle_q} \right\}.$$

We define $I = \lceil \log q \rceil$ and write

$$(4.1) \quad \mathcal{S}_{k,\ell,q}(\mathcal{A}; \mathcal{J}) \ll |\Sigma_0| + \sum_{i=1}^I |\Sigma_i|,$$

where

$$\begin{aligned} \Sigma_0 &= \sum_{m \in \mathbb{Z}_q} \sum_{\substack{x \in \mathbb{Z}_q^* \\ \langle x^\ell \rangle_q \leq q/N}} \alpha_m \gamma_x \mathbf{e}_q(mx^k), \\ \Sigma_i &= \sum_{m \in \mathbb{Z}_q} \sum_{\substack{x \in \mathbb{Z}_q^* \\ e^{i+1}q/N \geq \langle x^\ell \rangle_q > e^i q/N}} \alpha_m \gamma_x \mathbf{e}_q(mx^k), \quad i = 1, \dots, I. \end{aligned}$$

Now using Lemmas 3.2 and 3.3, we have

$$(4.2) \quad |\Sigma_0| \leq \|\mathcal{A}\|_2 N \sqrt{(q/N)q^{1+o(1)}} \leq \|\mathcal{A}\|_2 N^{1/2} q^{1+o(1)}.$$

Also, for $i = 1, \dots, I$, using that if $e^{i+1}q/N \geq \langle x^\ell \rangle_q > e^i q/N$ then $\gamma_x \ll N e^{-i}$, hence, again by Lemmas 3.2 and 3.3, we obtain

$$\begin{aligned} \Sigma_i &= \sum_{m \in \mathbb{Z}_q} \sum_{\substack{x \in \mathbb{Z}_q^* \\ e^{i+1}q/N \geq \langle x^k \rangle_q > e^i q/N}} \alpha_m \gamma_x \mathbf{e}_q(mx^\ell) \\ &\leq \|\mathcal{A}\|_2 (q^{o(1)} N^2 e^{-2i} e^i q/N)^{1/2} q^{1/2} = e^{-i/2} \|\mathcal{A}\|_2 N^{1/2} q^{1+o(1)}. \end{aligned}$$

Therefore,

$$(4.3) \quad \sum_{i=1}^I |\Sigma_i| \leq \|\mathcal{A}\|_2 N^{1/2} q^{1+o(1)} \sum_{i=1}^I e^{-i/2} \leq \|\mathcal{A}\|_2 N^{1/2} q^{1+o(1)}.$$

Combining (4.2) and (4.3), we obtain the first bound.

For the second bound we turn to use the method of [19]. For a fixed integer $\nu \geq 2$, using the Hölder inequality, we obtain

$$\begin{aligned} (4.4) \quad |\Sigma_0| &\leq \left(\sum_{m \in \mathbb{Z}_q} |\alpha_m| \right)^{1-1/\nu} \left(\sum_{m \in \mathbb{Z}_q} |\alpha_m|^2 \right)^{1/2\nu} W_0 \\ &= \|\mathcal{A}\|_1^{1-1/\nu} \|\mathcal{A}\|_2^{1/\nu} W_0, \end{aligned}$$

where

$$W_0 = \left(\sum_{m \in \mathbb{Z}_q} \left| \sum_{\substack{x \in \mathbb{Z}_q^* \\ \langle x^\ell \rangle_q \leq q/N}} \gamma_x \mathbf{e}_q(mx^k) \right|^{2\nu} \right)^{1/2\nu}.$$

Opening up the inner sum, changing the order of summation and using the orthogonality of exponential functions, we obtain

$$\begin{aligned}
W_0 &= \sum_{m \in \mathbb{Z}_q} \sum_{\substack{x_1, \dots, x_{2\nu} \in \mathbb{Z}_q^* \\ \langle x_i^\ell \rangle_{q \leq q/N, i=1, \dots, 2\nu}}} \prod_{j=1}^{\nu} \gamma_{x_j} \overline{\gamma_{x_{\nu+j}}} \mathbf{e}_q \left(m \sum_{j=1}^{\nu} (x_j^k - x_{\nu+j}^k) \right) \\
&= q \sum_{\substack{\langle x_i^\ell \rangle_{q \leq q/N, i=1, \dots, 2\nu} \\ x_1^k + \dots + x_\nu^k \equiv x_{\nu+1}^k + \dots + x_{2\nu}^k \pmod{q}}} \prod_{j=1}^{\nu} \gamma_{x_j} \overline{\gamma_{x_{\nu+j}}} \\
&\leq N^{2\nu} q \sum_{\substack{\langle x_i^\ell \rangle_{q \leq q/N, i=1, \dots, 2\nu} \\ x_1^k + \dots + x_\nu^k \equiv x_{\nu+1}^k + \dots + x_{2\nu}^k \pmod{q}}} 1.
\end{aligned}$$

Let $u_i = \langle x_i^\ell \rangle_q$, $v_i = x_i^k$, then we have

$$\begin{aligned}
v_1 + \dots + v_\nu &\equiv v_{\nu+1} + \dots + v_{2\nu} \pmod{q}, \\
u_i^k &\equiv \pm v_i^l \pmod{q}, \quad 0 < u_i \leq q/N.
\end{aligned}$$

Applying Lemma 3.4, we have

$$W_0 \leq N^{2\nu} q^{1+o(1)} \left(\left(\frac{q}{N} \right)^{2\nu} q^{-1} + \left(\frac{q}{N} \right)^{2\nu^2/(\nu+1)} \right).$$

Then, we see from (4.4)

$$|\Sigma_0| \leq \|\mathcal{A}\|_1^{1-1/\nu} \|\mathcal{A}\|_2^{1/\nu} \left(q + q^{(2\nu^2+\nu+1)/2\nu(\nu+1)} N^{1/(\nu+1)} \right) q^{o(1)}.$$

Similarly, we also obtain

$$|\Sigma_i| \leq \|\mathcal{A}\|_1^{1-1/\nu} \|\mathcal{A}\|_2^{1/\nu} \left(q + q^{(2\nu^2+\nu+1)/2\nu(\nu+1)} N^{1/(\nu+1)} e^{-i/(\nu+1)} \right) q^{o(1)},$$

and the result now follows from (4.1).

4.2. **Proof of Theorem 2.3.** By the Cauchy inequality we have

$$\begin{aligned}
|\mathcal{S}_{k,p}^*(\mathcal{A}, \mathcal{B}; \mathcal{J})|^2 &\leq \|\mathcal{A}\|_2 \|\mathcal{B}\|_2 \sum_{n \in \mathcal{J}} \sum_{m \in \mathbb{Z}_p} \left| \sum_{x \in \mathbb{Z}_p^*} \mathbf{e}_p(mx^k + nx^{-1}) \right|^2 \\
&= \|\mathcal{A}\|_2 \|\mathcal{B}\|_2 \sum_{n \in \mathcal{J}} \sum_{m \in \mathbb{Z}_p} \left| \sum_{x \in \mathbb{Z}_p^*} \mathbf{e}_p(mx^{-k} + nx) \right|^2 \\
&= \|\mathcal{A}\|_2 \|\mathcal{B}\|_2 \sum_{n \in \mathcal{J}} \sum_{m \in \mathbb{Z}_p} \sum_{x, y \in \mathbb{Z}_p^*} \mathbf{e}_p(m(x^{-k} - y^{-k}) + n(x - y)).
\end{aligned}$$

Now, writing $y = x + z$ we obtain

$$\begin{aligned}
|\mathcal{S}_{k,p}^*(\mathcal{A}, \mathcal{B}; \mathcal{J})|^2 &\leq \|\mathcal{A}\|_2 \|\mathcal{B}\|_2 \sum_{n \in \mathcal{J}} \sum_{m \in \mathbb{Z}_p} \sum_{x \in \mathbb{Z}_p^*} \sum_{z \in \mathbb{Z}_p^* - x} \mathbf{e}_p(m(x^{-k} - (x+z)^{-k}) - nz),
\end{aligned}$$

where $\mathbb{Z}_p^* - x = \{z \in \mathbb{Z}_p : z + x \in \mathbb{Z}_p^*\}$. Changing the order of summation and applying Lemma 3.1, we obtain

(4.5)

$$|\mathcal{S}_{k,p}^*(\mathcal{A}, \mathcal{B}; \mathcal{J})|^2 \ll \|\mathcal{A}\|_2 \|\mathcal{B}\|_2 \sum_{x \in \mathbb{Z}_p^*} \sum_{m \in \mathbb{Z}_p} \left| \sum_{z \in \mathbb{Z}_p^* - x} \eta_z \mathbf{e}_p(m(x+z)^{-k}) \right|,$$

where

$$|\eta_z| \leq \min \left\{ N, \frac{p}{\langle z \rangle_p} \right\}.$$

For every fixed x , to estimate

$$W(x) = \sum_{m \in \mathbb{Z}_p} \left| \sum_{z \in \mathbb{Z}_p^* - x} \eta_z \mathbf{e}_p(m(x+z)^{-k}) \right|,$$

we now set $I = \lceil \log(p/2) \rceil$ and define $2(I+1)$ sets

$$\begin{aligned}
\mathcal{Z}_0^\pm &= \{z \in \mathbb{Z} : p/N \geq \pm z > 0\}, \\
\mathcal{Z}_i^\pm &= \{z \in \mathbb{Z} : \min\{p/2, e^i p/N\} \geq \pm z > e^{i-1} p/N\}, \quad i = 1, \dots, I.
\end{aligned}$$

Then

$$(4.6) \quad W(x) \ll \sum_{i=0}^I |T_i^\pm(x)|,$$

where

$$T_i^\pm(x) = \sum_{m \in \mathbb{Z}_p} \left| \sum_{z \in (\mathbb{Z}_p^* - x) \cap \mathcal{Z}_i^\pm} \eta_z \mathbf{e}_p(m(x+z)^{-k}) \right|, \quad i = 0, \dots, I.$$

For a fixed positive integer ν , using again the Hölder inequality, we obtain

$$\begin{aligned} |T_i(x)^\pm|^{2\nu} &\leq p^{2\nu-1} \sum_{m \in \mathbb{Z}_p} \left| \sum_{z \in (\mathbb{Z}_p^* - x) \cap \mathcal{Z}_i^\pm} \eta_z \mathbf{e}_p(m(x+z)^{-k}) \right|^{2\nu} \\ &= p^{2\nu-1} \sum_{z_1, \dots, z_{2\nu} \in (\mathbb{Z}_p^* - x) \cap \mathcal{Z}_i^\pm} \prod_{j=1}^{\nu} \overline{\eta_{z_j} \eta_{z_{\nu+j}}} \\ &\quad \sum_{m \in \mathbb{Z}_p} \mathbf{e}_p \left(m \sum_{j=1}^{\nu} ((x+z_j)^{-k} - (x+z_{\nu+j})^{-k}) \right). \end{aligned}$$

So, denoting by $\Omega_i^\pm(x)$ the following set

$$\Omega_i^\pm(x) = \left\{ (z_1, \dots, z_{2\nu}) \in (\mathcal{Z}_i^\pm)^{2\nu} : \sum_{j=1}^{2\nu} \frac{(-1)^j}{(x+z_j)^k} \equiv 0 \pmod{p} \right\}$$

we can now see that

$$\begin{aligned} |T_i^\pm(x)|^{2\nu} &\leq p^{2\nu} \sum_{(z_1, \dots, z_{2\nu}) \in \Omega_i^\pm(x)} \prod_{j=1}^{\nu} \overline{\eta_{z_j} \eta_{z_{\nu+j}}} \\ &\ll (e^{-i}N)^{2\nu} p^{2\nu} \#\Omega_i^\pm(x), \end{aligned}$$

where we have used

$$|\eta_z| \ll e^{-i}N, \quad i = 0, \dots, I.$$

Applying Lemma 3.5, we have

$$\begin{aligned} |T_i^\pm(x)|^{2\nu} &\leq (e^{-i}N)^{2\nu} p^{2\nu+o(1)} \left(\left(e^i \frac{p}{N} \right)^{2\nu} p^{-1} + \left(e^i \frac{p}{N} \right)^{2\nu^2/(\nu+1)} \right) \\ &= \left(p^{4\nu-1} + p^{(4\nu^2+2\nu)/(\nu+1)} N^{2\nu/(\nu+1)} e^{-2\nu i/(\nu+1)} \right) p^{o(1)}. \end{aligned}$$

Then

$$(4.7) \quad |T_i^\pm(x)| \leq \left(p^{(4\nu-1)/(2\nu)} + p^{(2\nu+1)/(\nu+1)} N^{1/(\nu+1)} e^{-i/(\nu+1)} \right) p^{o(1)}.$$

The result now follows from (4.5), (4.6) and (4.7).

4.3. Proof of Theorem 2.4. We consider only the integers $q \in [Q, 2Q]$ for which the bound of Corollary 3.8 holds. Now, proceeding as in the proof of the second bound in Theorem 2.1 but use Corollary 3.8 instead of Lemma 3.4.

5. COMPARISON WITH PREVIOUS RESULTS

We note that for a prime $q = p$, in our notation for the functions $K_1(t)$ and $K_2(t)$ from [14] we have

$$K_1(mn) = p^{-1/2} S_{-2,1,p}(ab^2 m^2, n) = p^{-1/2} S_{2,-1,p}(ab^2 m^2, n)$$

and

$$K_2(mn^2) = p^{-1/2} S_{-2,1,p}(ab^2 m, n) = p^{-1/2} S_{2,-1,p}(ab^2 m, n).$$

Recalling the definition (1.1), we now see that the results of Nunes [14] can be written as

$$(5.1) \quad \mathcal{S}_{2,p}^*(\mathcal{A}; \mathcal{M}_1, \mathcal{J}) \leq \sqrt{\|\mathcal{A}\|_1 \|\mathcal{A}\|_2} p^{3/4+o(1)} M^{1/16} N^{5/8}$$

provided that $1 \leq M \leq N^2$ and $MN^2 \leq p^2$ and also

$$(5.2) \quad \mathcal{S}_{2,p}^*(\mathcal{A}; \mathcal{M}_2, \mathcal{J}) \leq \sqrt{\|\mathcal{A}\|_1 \|\mathcal{A}\|_2} p^{3/4+o(1)} M^{1/12} N^{7/12}$$

provided that $1 \leq M \leq N^2$ and $MN \leq p^{3/2}$, where

$$\mathcal{M}_1 = \{\alpha j : j = 1, \dots, M\} \quad \text{and} \quad \mathcal{M}_2 = \{\alpha j^2 : j = 1, \dots, M\}$$

(with some $\alpha \in \mathbb{F}_p^*$) and \mathcal{J} is an interval of length $N < p$. Using Theorem 2.1 with $\nu = 2$ (and recalling that its bound does not depend on the support \mathcal{M} of the weights \mathcal{A} , see (1.5)), we obtain

$$\mathcal{S}_{2,p}^*(\mathcal{A}; \mathcal{M}_j, \mathcal{J}) \leq \sqrt{\|\mathcal{A}\|_1 \|\mathcal{A}\|_2} (p + p^{11/12} N^{1/3}) p^{o(1)}, \quad j = 1, 2.$$

This bound improves (5.1) for

$$MN^{10} \geq p^{4+\varepsilon} \quad \text{and} \quad M^3 N^{14} \geq p^{8+\varepsilon}$$

and improves (5.2) for

$$MN^7 \geq p^{3+\varepsilon} \quad \text{and} \quad MN^3 \geq p^{2+\varepsilon}$$

with some fixed $\varepsilon > 0$. In particular, if M and N are of similar sizes, that is, $N = M^{1+o(1)}$, this happens for $M \geq p^{8/17+\varepsilon}$ and $M \geq p^{1/2+\varepsilon}$, respectively.

We further note that for applications to smooth numbers in arithmetic progressions only the bound (5.1) matters and only in the case of constant weights and thus it has to be compared with that of Corollary 2.2 (it is easy to see that for $\ell = 1$ it can be extended to the set $\mathcal{M}_1 = \alpha \mathcal{I}$). In particular, in this case the bound (2.1) is better when

$$M^{13} N^{-2} \geq p^{4+\varepsilon} \quad \text{and} \quad M^{23} N^{-6} \geq p^{8+\varepsilon},$$

or similarly with M and N can be interchanged, see also (2.2) for the range when it is nontrivial.

In particular, in the critical for applications regime, when $N = M^{1+o(1)}$, the bound (2.1) is both better and nontrivial for $M \geq p^{8/17+\varepsilon}$. However, the potential improvement of [14], which is implied by our bounds seems to be of the same strength as in the follow up work of Nunes [15], where this is achieved via a different approach.

ACKNOWLEDGEMENT

The authors are grateful to Ramon Nunes for very useful discussions, in particular for the information about his results in [15] and their comparison with potential improvements coming from our new bounds.

The first and the third authors gratefully acknowledge the support, hospitality and excellent conditions of the School of Mathematics and Statistics of UNSW during their visit.

This work was supported by NSFC Grant 11401329 (for K. Liu), by ARC Grant DP140100118 (for I. E. Shparlinski) and by the Natural Science Foundation of Shaanxi Province of China Grant 2016JM1017 (for T. P. Zhang).

REFERENCES

- [1] V. Blomer, É. Fouvry, E. Kowalski, P. Michel and D. Milićević, ‘On moments of twisted L -functions’, *Amer. J. of Math.*, (to appear).
- [2] V. Blomer, É. Fouvry, E. Kowalski, P. Michel and D. Milićević, ‘Some applications of smooth bilinear forms with Kloosterman sums’, *Proc. Steklov Math. Inst.*, (to appear).
- [3] J. Bourgain and M. Z. Garaev, ‘Sumsets of reciprocals in prime fields and multilinear Kloosterman sums’, *Izv. Ross. Akad. Nauk Ser. Mat.*, **78** (2014), 9–72 (in Russian); translation in *Izv. Math.*, **78** (2014), 656–707.
- [4] É. Fouvry, E. Kowalski and P. Michel, ‘Algebraic trace functions over the primes’, *Duke Math. J.*, **163** (2014), 1683–1736.
- [5] É. Fouvry and I. E. Shparlinski, ‘On a ternary quadratic form over primes’, *Acta Arith.*, **150** (2011), 285–314.
- [6] J. B. Friedlander and H. Iwaniec, ‘The divisor problem for arithmetic progressions’, *Acta Arith.*, **45** (1985), 273–277.
- [7] D. R. Heath-Brown, ‘The least square-free number in an arithmetic progression’, *J. Reine Angew. Math.*, **332** (1982), 204–220.
- [8] M. N. Huxley, ‘A note on polynomial congruences’, *Recent Progress in Analytic Number Theory, Vol.1*, Academic Press, 1981, 193–196.
- [9] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society, Providence, RI, 2004.
- [10] A. A. Karatsuba, ‘Analogues of Kloosterman sums’, *Izv. Ross. Akad. Nauk Ser. Mat. (Transl. as Russian Acad. Sci. Izv. Math.)*, **55**(5) (1995), 93–102 (in Russian)

- [11] R. Khan, ‘The divisor function in arithmetic progressions modulo prime powers’, *Mathematika*, **62** (2016), 898–908.
- [12] E. Kowalski, P. Michel and W. Sawin, ‘Bilinear forms with Kloosterman sums and applications’, *Preprint*, 2015 (available from <http://arxiv.org/abs/1511.01636>).
- [13] K. Liu, I. E. Shparlinski and T. P. Zhang, ‘Divisor problem in arithmetic progressions modulo a prime power’, *Preprint*, 2016 (available from <http://arxiv.org/abs/1602.03583>).
- [14] R. M. Nunes, ‘Squarefree numbers in large arithmetic progressions’, *Preprint*, 2016 (available from <http://arxiv.org/abs/1602.00311>).
- [15] R. M. Nunes, ‘A note on the least squarefree number in an arithmetic progressions’, *Preprint*, 2016 (available from <http://arxiv.org/abs/1605.03347>).
- [16] L. B. Pierce, ‘The 3-part of class numbers of quadratic fields, *J. London Math. Soc.*, **71** (2005), 579–598.
- [17] O. Roche-Newton, M. Rudnev and I. D. Shkredov, ‘New sum-product type estimates over finite fields’, *Adv. Math.*, **293** (2016), 589–605.
- [18] I. E. Shparlinski, ‘On exponential sums with sparse polynomials and rational functions’, *J. Number Theory*, **60** (1996), 233–244.
- [19] I. E. Shparlinski, ‘Bilinear forms with Kloosterman and Gauss sums’, *Preprint*, 2016 (available from <http://arxiv.org/abs/1608.06160>).
- [20] I. E. Shparlinski and T. P. Zhang, ‘Cancellations amongst Kloosterman sums’, *Acta Arith.*, **176** (2016), 201–210.
- [21] D. Suryanarayana and R. Sitaramachandra Rao, ‘The distribution of squarefull integers’, *Arkiv för Matematik*, **11** (1973), 195–201.
- [22] J. Wu and P. Xi, ‘Arithmetic exponent pairs for algebraic trace functions and applications’, *Preprint*, 2016 (available from <http://arxiv.org/abs/1603.07060>).
- [23] P. Xi (with an appendix by É. Fouvry, E. Kowalski and P. Michel), ‘Large sieve inequalities for algebraic trace functions’, *Intern. Math. Res. Notices*, (to appear).
- [24] I. M. Vinogradov, *Elements of number theory*, Dover Publ., NY, 1954.

SCHOOL OF MATHEMATICS AND STATISTICS, QINGDAO UNIVERSITY, No.308,
 NINGXIA ROAD, SHINAN, QINGDAO, SHANDONG, 266071, P. R. CHINA
E-mail address: liukui@qdu.edu.cn

DEPARTMENT OF PURE MATHEMATICS, UNIVERSITY OF NEW SOUTH WALES,
 SYDNEY, NSW 2052, AUSTRALIA
E-mail address: igor.shparlinski@unsw.edu.au

SCHOOL OF MATHEMATICS AND INFORMATION SCIENCE, SHAANXI NORMAL
 UNIVERSITY, XI’AN 710019 SHAANXI, P. R. CHINA
E-mail address: tpzhang@snnu.edu.cn